暗号化を阻む政府の動きに抗して

暗号技術はオンラインのコミュニケーションで安全を確保するための必須の手段です。暗号化とは、データを人間には理解できない記号群に置き換えること で読まれないように対処する技術ですが、通信のデータに人間がアクセスする ときには、人間が読むことのできるデータとして表示されるので、暗号化の実 際を直感的に把握する場面にはほとんど遭遇しないかもしれません。その結果 として暗号化が果している役割は、家の玄関に鍵をかけることに比べても、そ の効果や役割を実感しづらく、暗号化への対処が疎かになりがちです。

暗号化には、ネットの回線上のデータは暗号化されるがプロバイダーのサーバー などでは暗号化されずに保存される場合と、プロバイダーですら通信の内容を 読むことができず、発信者と宛先の受信者双方だけが読むことのできる場合が あります。後者のような場合をエンド・ツー・エンド暗号化と呼び、より一層 プライバシー保護にとっては好ましいものになります。

他方で、通信への監視をより一層強化したいと考えている政府や企業のなかに は、私たちが自由に暗号化のツールを利用できるということを快く思っていな い場合があることも知られています。米国、英国、 EU 、そして日本などの政府 は、テロ、子どもの性的虐待、薬物犯罪などの犯罪捜査で暗号化の弱体を狙っ ており、ロシア、中国、エジプトなどの政府は、反政府言論の取り締まり目的 のために暗号化を禁止するなどの措置へと動いています。

今回のこのセミナーでは、暗号化のなかでも特に重要性を増しているエンド・ ツー・エンド暗号化を中心に、その仕組みを概説するとともに、政府などが画 策しているエンド・ツー・エンド暗号化を弱体化しようとする動きについても 紹介します。

グローバル暗号化デー

https://www.globalencryption.org/2024/07/global-encryption-day-2024/

Global Encryption Day 2024

Online, 21 October 2024

Hosted by Global Encryption Coalition

Save the date! Join us on 21 October 2024 for the 4th annual Global Encryption Day.

- Register and participate at Encrypt Today to Safeguard Tomorrow: The Encryption Summit
- Organize an event for the Global Encryption Day 2024
- Participate in an event organized in your part of the world or online
- Revisit Global Encryption Day 2023
- Hear stories about how encryption empowers and protects people
- Tell us your story about why you stand up for strong encryption
- Become a Friend of the Coalition (for individuals) or a Member (for organizations)
- Follow us on X and Facebook

グローバル暗号化デー

Celebrating your Digital Privacy on Global Encryption Day

Global Encryption Day is October 21, and the Institute for Policy Innovation (IPI) invites you to join our virtual briefing

When: 21 October 2024

Where: Virtual

In opposition to government moves to restrict encryption

Cryptography is an essential means of ensuring security in online communication. Cryptography is a technology that makes data unreadable by

When: 21 October 2024

Where: Japan

CAMPAIGN FOR YOUTH PARTICIPATION ON ONLINE SECURITY

The event is a CAMPAIGN FOR YOUTH PARTICIPATION IN ONLINE SECURITY. The program, commemorating Global Encryption Day 2024, will look

When: 21 October 2024

Where: American Corner, Jigawa State.

Global Encryption Day San Francisco

Global Encryption Day (GED) is an annual event organized by the Global Encryption Coalition (GEC), designed to raise awareness about

When: 21 October 2024

Global Encryption Day 2024

Save the date! Join us on 21 October 2024 for the 4th annual Global Encryption Day. Register and participate at

When: 21 October 2024

Where: Online

Kwara Global Encryption Day 2024 Summit

The "Kwara Global Encryption Day 2024 Summit" is an initiative by the Webfala Digital Skills for all Initiative to mark

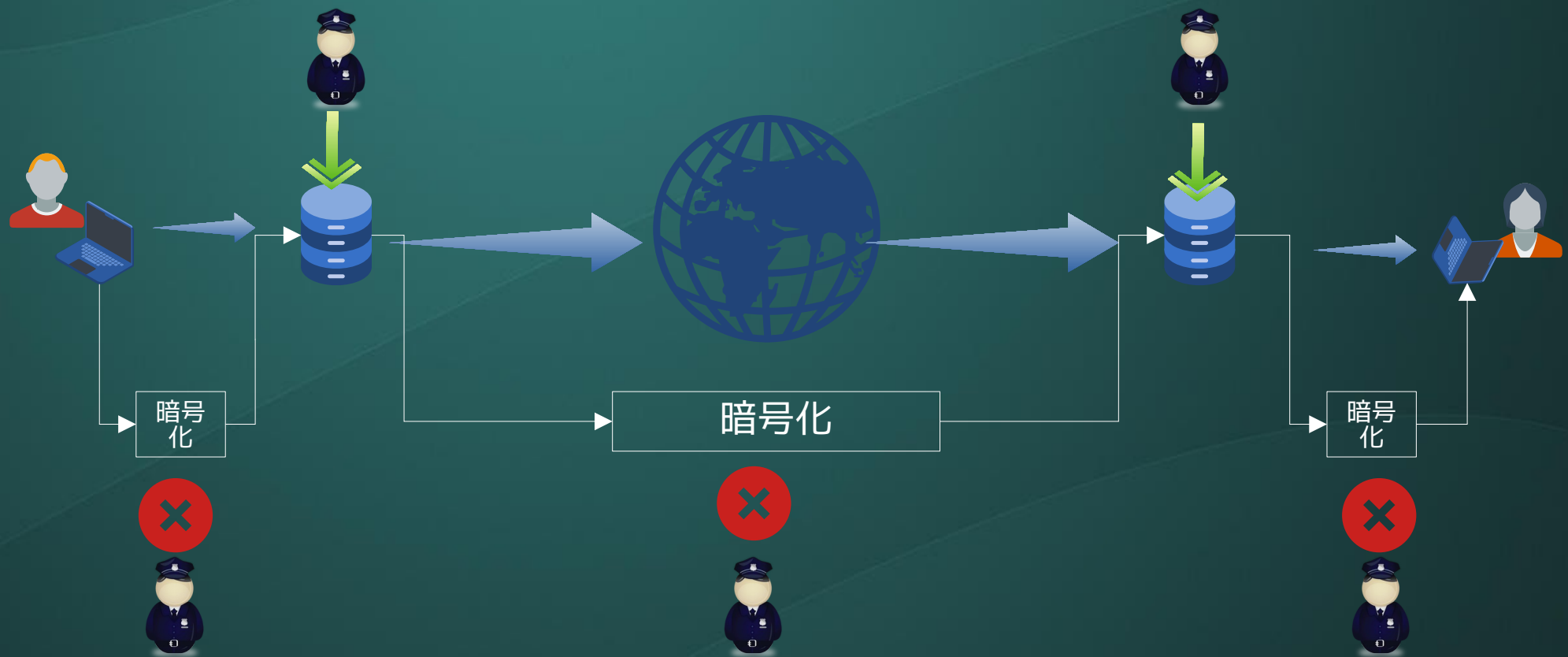
When: 24 October 2024

Where: Ilorin. Kwara state,

暗号化とは

通常よく言われる「暗号化」では、下図のように、通信の経路では通信の内容が暗号化されるが、契約しているプロバイダーのサーバーではデータが暗号化されないままになる。メールであれば、プロバイダーは契約者が送受信するメールを読むことが可能になる。

従来の暗号化ではサーバーが狙われる

- 通信経路は暗号化されているためにデータを取得しても読むことができない
- 唯一可読となるのはプロバイダーのサーバーとなる

エンド・ツーエンド暗号化とは

エンド・ツーエンド暗号化は、通信の末端(エンド)同士を暗号化されたままで繋ぐ仕組みになる。プロバイダーのサーバーでも暗号化が維持されるので、プロバイダーも通信の内容を読むことができない。誰もいない原っぱで二人きりで話すような環境を作ること。

エンド・ツー・エンド暗号化

- E2EE は、私たちが干渉されることなくコミュニケーションできて自分をより高めるための安全でプライベートな空間へのアクセスを提供する。
- 私たちを犯罪者から守ってくれる。
- 不必要で不釣り合いな監視から私たちを守ってくれるジャーナリスト、デモ参加者、政治的反体制派、人権擁護活動家など、強大な権力に異議を唱えようとする人々にとっても不可欠である。
- E2EE は、表現の自由や意見の自由など、プライバシーを超えた人権の行使を促進する。このような空間は、私たち全員にとって必要なのである。

エンド・ツー・エンド暗号化

政府や捜査機関などは暗号化されたデータを読むことを可能にしたがっている。その言い分は、

- 犯罪捜査に欠かせない証拠である
- 捜査機関が暗号を解読できたとしても一般人のプライバシーを侵害することはない仕組みを導入できる

最近の報道でも、犯罪に秘匿性の高いアプリが用いられていることが繰り返し報じられている。報道では、あたかも秘匿性の高いアプリが、私たちのプライバシーは言論の自由の権利に必須である点に言及していない。その結果秘匿性の高いアプリの利用を控える萎縮効果も生まれている可能性がある。

暗号の「鍵」

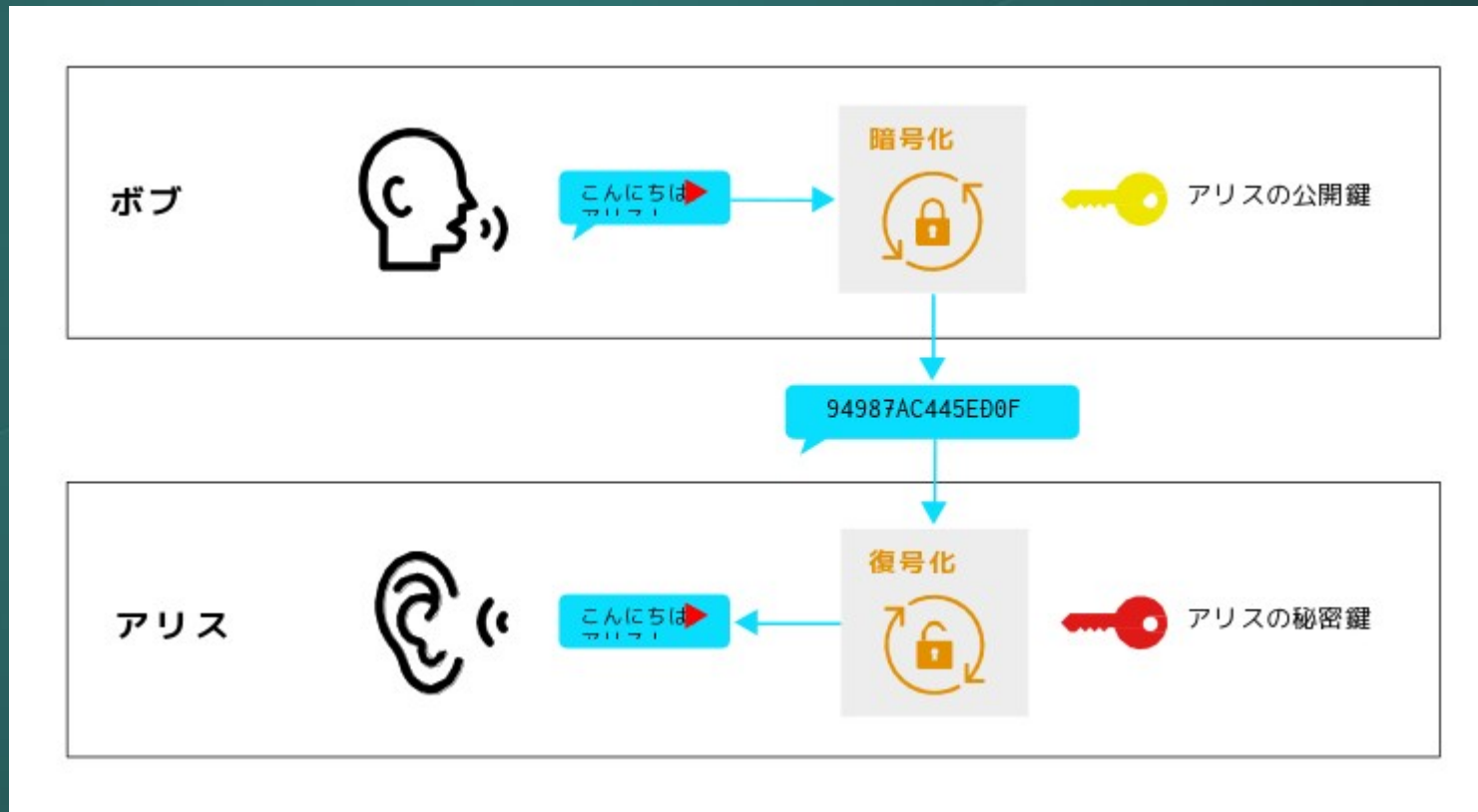
鍵とは、

- 人間が読むことのできるデータを暗号化する
- 暗号化されたデータを人間が読むことができるデータにする

たとえば、暗号文「 dloW olloH 」の鍵は「後ろから読む」

dloW olloH ⇒ Hello Wold

この鍵を知っている者だけが、暗号を解読できる。暗号を解読することを「復号化」と呼ぶ。

欠点：「鍵」を共有しなければ暗号を解読できない。どうやって共有するのかが難しい。

暗号の「鍵」

公開鍵と秘密鍵：アリスにボブがメッセージを送る

- ボブはアリスの「公開鍵」でメッセージを暗号化
- アリスは暗号化されたメッセージを自分の「秘密鍵」で復号

※ 実際のやりとりはもっと複雑です

暗号の「鍵」

公開鍵と秘密鍵 (資料 p.4 ～ 5)

- 公開鍵：「暗号化はできても復号できない鍵」 自分宛にメッセージを送る人達誰にでも渡して構わない鍵。この鍵を使って自分宛に暗号化されたメッセージを送ってもらう。
- 秘密鍵：「暗号を復号するために使う鍵」 絶対に他人に知らてはいけない内緒の鍵。この鍵を使って自分宛に来た暗号化されたメッセージを復号する。

実空間で一般に用いられている鍵は、「鍵をかける」こともできるし「鍵を開ける」こともできる鍵になる。こうした鍵は「共通鍵」と呼ばれる。共通鍵は、メッセージの送り手と受け手で鍵を共有しなければならなず、しかもこの鍵を第三者に盗まれてしまうと、「開ける」ことが可能になってしまう。この欠点を「公開鍵暗号方式」は、鍵をかけることはできても開けることのできない鍵、という発想で解決した。

エンド・ツー・エンド(E2EE) 暗号化

E2EEでは、ユーザーは自分のデバイス(パソコンやスマホ)上でメッセージの内容を暗号化し、メッセージングサービスやアプリケーションはその暗号化されたメッセージの暗号化を最終的な受信者に送信する。送受信されるメッセージの暗号化と復号化はユーザーのデバイス上で行われるため、E2EE は目的とされた受信者だけがメッセージの内容にアクセスでき、通信サービスプロバイダーもアクセスできず安全である。

※しかし、もし「秘密鍵」が盗まれてしまったら、この鍵を使って暗号化された過去のデータも復号可能になってしまう。このリスクを防ぐ仕組みが「前方秘匿性」という仕組みである(資料p.5参照)

参考：https://xtech.nikkei.com/atcl/nxt/column/18/02306/121900004/

E2EEに関する重要な注意点

E2EEはメッセージのコンテンツのみを保護する
WhatsAppのような通信サービスプロバイダは、メッセージに付随するメタデータ（日付、送信者、受信者など）を見ることができる。このメタデータからプライバシーが明らかになる可能性がある。
したがって、E2EEは完全にプライベートな通信ソリューションではない。
E2EEを検討しているユーザーは、付随するメタデータから何が分かるのか、また、サービスプロバイダー、強制力を行使できる政府、違法な手段で入手しようとする犯罪者など、誰がメタデータにアクセスできる可能性があるのかを認識しておく必要がある。

E2EE の人権への影響

- 通信には多くの事業者が関与している。
- これらの事業体もまた通信を覗き見している可能性がある。
- E2EE は、メタデータを別にすればメッセージの本文は暗号化されるために、通信事業者も覗き見できない。この意味で E2EE は、あらゆるスパイの介入を「排除」し、私たちの通信をより安全なものにするのに役立つ。

E2EE の人権への影響

国連：2015年、暗号化の自由に関する分析

- 暗号化と匿名化は、意見や信条を保護するためのプライバシー領域を作り出す
- 敵対的な政治的、社会的、宗教的、法的環境においては特に重要
- 国家の検閲を回避し、当局の干渉を受けることなく情報や思想にアクセスすることができる
- ジャーナリスト、研究者、弁護士、市民社会は、自分自身（および情報源、クライアント、パートナー）を監視や嫌がらせから守る
- ジェンダー、宗教、エスニシティ、出身国、セクシュアリティといったアイデンティティの基本を探求する上で必須

E2EEの人権への影響

E2EEは、政府、企業、犯罪者による違法なプライバシー侵害から人々を守る手段になる。特にリスクが高いのは以下のような人々だ。

- その活動を強く否定する国において当の政治活動家を報道する**ジャーナリスト**。
- 権威主義体制に反対する**人権擁護活動家や政治活動家**。
- 政府の政策や行為に反対するデモ**参加者**。
- 同性愛が犯罪とされている国の**LGBTQIA+コミュニティのメンバーたち**。

※「誰がE2EEから恩恵を受けるのか？」p.10参照

E2EEの人権への影響

E2EEのユーザーは、いったい誰から身を守っているのだろうか？

- E2EEは<u>通信サービス提供す企業</u>でも、通信の内容を読めない

  ※E2EEではないサービスの場合、企業は目的の受信者にデータを渡す前に、暗号化されていない通信内容を彼らのサーバーに保存することができる。このような企業は、そのデータを他の用途に利用することができる。

- E2EEは<u>企業データにアクセスする悪意ある行為者</u>からも保護できる。

  ※Twitterの元従業員が、暗号化されていないTwitterデータへのアクセス権を悪用し、高級時計と数十万ドルと引き換えに、政治的反体制派の個人データを収集してサウジアラビアに渡した。

サービス・プロバイダーもまた、ハッキング[40]やデータ漏洩にさらされる。コンテンツが企業サーバーに保存されていたり、企業ネットワークを無防備に通過していたりすると、犯罪者や故意に攻撃する第三者にとっては攻撃可能な場所が一つ増えることになる。

E2EE の人権への影響

国家の監視(1)

- 国家が法的手続きを通じてサービスプロバイダーのコンテンツへのアクセスを直接求めることがより頻繁に起きている。
  - 通信内容の提出を要求する令状や命令がサービスプロバイダに送達される
  - コンテンツへの捜査機関による直接アクセスを提供するようサービスプロバイダに圧力をかける
- E2EEを使用するということは、サービスプロバイダがこのような要求に対して引き渡さなければならないコンテンツを持たないことを意味する。

E2EE の人権への影響

国家の監視(2)

政府によっては、主要な通信ケーブルを流れるすべての通信内容を傍受したり、サービスプロバイダにすべての通信内容の提出を義務づけたりするような、大規模な監視も行っている。[43] E2EEは、大量傍受という点ではこれを実質的に無意味なものし、企業サーバーからコンテンツを削除して政府が企業コンテンツへの大量アクセスを求めた場合でも引き渡すコンテンツを残さないようにして、転送中のメッセージ・コンテンツを暗号化することで大量監視を軽減するサービスを提供する。

プライバシー権と公共の利益

たとえば秘匿性の高い通信アプリを利用することは、プライバシーの権利を保護する上で必須だ。しかし、他方で、犯罪捜査のためにプライバシーの権利を一定程度制限することも認められている。(たとえば、家宅捜索や身体検査など、裁判所の令状があれば適法な捜査の権限となる)
同様に、通信についても、秘匿性の高いサービスを制限することをも場合によっては認められるべきかどうかが問題になる。たとえば、何らかの方法で、暗号データの復号化を可能にしたり、暗号データが復号化された時点でデータを取得するなどの手法を認めるかどうか、である。
この点については、人権団体や国連の人権機関は一致して、暗号化を弱体化させるような制度の導入の影響の重大性を強調し、弱体化という選択肢を否定している。

国家による E2EE へのアクセス

現状

米国、英国、EU、のような一部の政府は、テロ、子どもの性的虐待、薬物犯罪などの犯罪捜査を推進するために、法執行機関や諜報機関が使用することを目的としたアクセスを促進してきた。

ロシア、中国、エジプトのような他の政府は、しばしば反対意見の取り締まりのような非合法な目的のために、アクセスを維持するために、暗号化を全面的に禁止することを事実上求めている。

国家による E2EE へのアクセス

<u>争点</u>

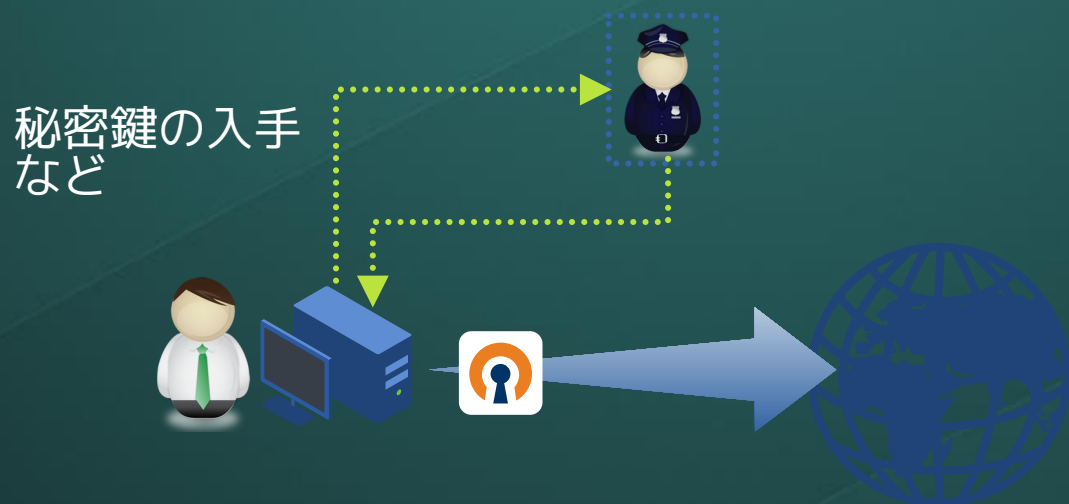
テロや子どもの搾取といった重大犯罪の防止は、通信にアクセスする重要かつやむを得ない理由になりうる。

しかし

- 重大な犯罪の疑いのある個人のE2EE通信に、法執行機関やその他の正当な政府だけがアクセスできるようにする方法はない。
- 重大犯罪捜査でE2EE通信のセキュリティを弱めた場合
- 十分な技術力をもつ行為者にとってはアクセス可能な脆弱性となる。
- 特定の捜査対象者だけでなく、サービスプロバイダーの全ユーザーのセキュリティを「破る」ことになる。

国家による E2EE へのアクセス
事例：バックドア

送信者や受信者の知らないところで許可なしに、第三者が通信にアクセスすることを可能にするもの

参加者の秘密鍵を入手したり、暗号化アルゴリズムに関する秘密の知識を持っていて、その解法が想定よりも簡単になるような方法——例えば、他の方法では見られない数学的欠陥など——を利用したり、量子コンピューターの能力を利用するなどして、大きな素数の因数分解を、現在のブルートフォース（総当り）のアプローチよりも数学的に簡単にする革新的な方法を見つけることによって行うことができる。

国家によるE2EEへのアクセス
事例：キーエスクロー

バックドアの一種である。

1990年代半ば、法執行機関は暗号化に対抗措置を提案

ある鍵でデータが暗号化された場合、政府が将来、送信されたデータにアクセスする場合に備えて、この鍵を「信頼できる」サードパーティ当局に登録（復元を許可するか、さもなければ預託）する義務があるというもの。

現代では頻繁に暗号鍵を生成しなおすことでセキュリティを確保しているため、長期にわたって同じ鍵を用いることを前提とするキーエスクローは時代状況に逆行し、安全性を損う。

国家による E2EE へのアクセス
事例：ダウングレード攻撃

より安全性の低い暗号化方式、例えば現代の計算能力で簡単に破れるような暗号化方式の使用を強制することである。一般的に、暗号鍵が長ければ長いほど、暗号化された通信を破り解読するのは難しくなる。

中国のようないくつかの国では、暗号キーに使用できる文字数を指定している。例えば、標準的な2048ビットの鍵長に対し、64文字（または「ビット」）の鍵長の場合、秘密鍵の「方程式」をより容易により少ない時間と計算能力で解くことができる。

これは、ユーザーにはより安全でない通信方法を使用させ、秘密鍵を簡単に入手することで結果としてバックドアを作るダウングレード攻撃である。

強力な暗号を違法化

国家による E2EE へのアクセス 事例：ゴースト・プロトコル

2018年、英国のスパイ機関GCHQの提案

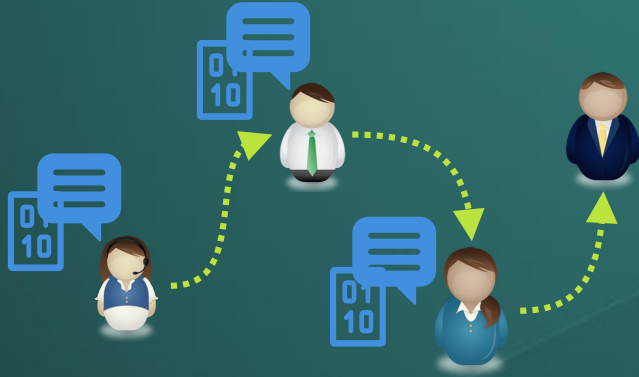
サービスプロバイダーは、E2EE会話をホストする際に、目に見えない参加者（一部ではゴーストと呼ばれている）を会話に追加する義務を負うようにすべきだというもの。後日、会話の監視が必要となった場合、法執行機関は、その見えない参加者として会話にアクセスすることができる。

- ユーザーは誰が会話に参加しているのか確認できなくなることを意味している。
- 人権を尊重する法執行機関によって、意図したとおりに標的を絞った捜査に使用されるかもしれないが、犯罪者に悪用されたり、不当な目的を持った国家に利用されたりする可能性もある。

国家によるE2EEへのアクセス
事例：メッセージ・ハッシュ・エスクロー

インド政府はE2EEに大きな懸念

特にWhatsAppのようなE2EEシステム内で転送される口コミコンテンツの「発信者」を追跡できるようにしたいと考えて考案された手段。

SNSのメッセージの最初の発信者が誰を特定する手法。

この方法には技術的な難点があるが、政府がこのシステムを導入する目的は、E2EE通信の内容を明らかにすることにあり、結果としてE2EEを破ることになる。

国家によるE2EEへのアクセス事例：クライアントサイド・スキャン

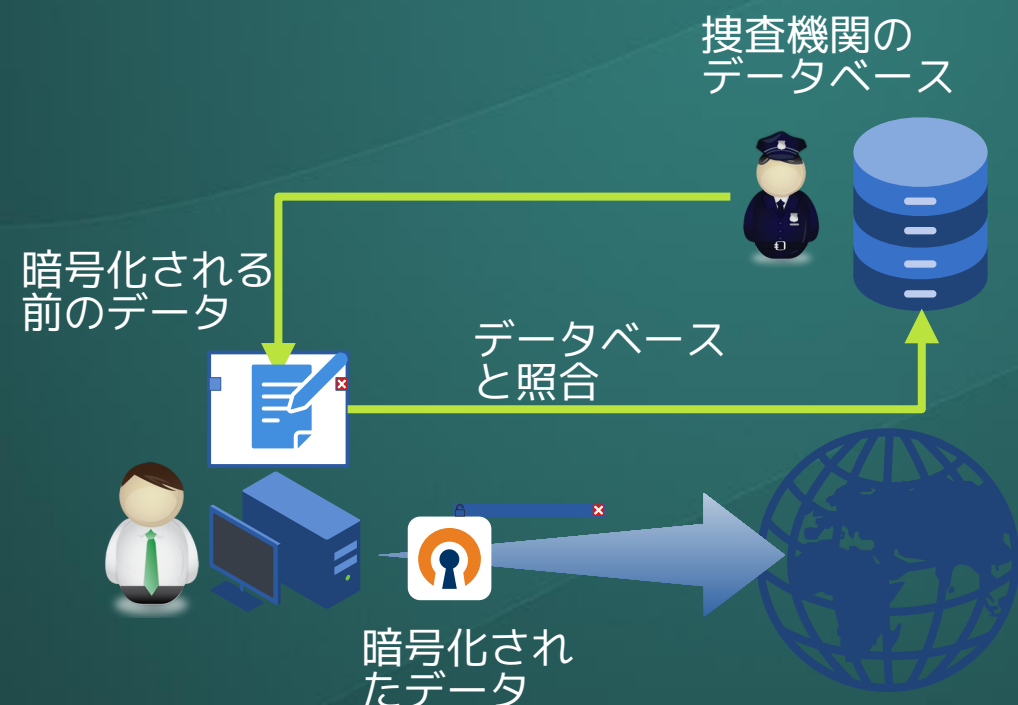
暗号化前または暗号化解除後に、通信の一報の側でデバイス上のコンテンツをスキャンすることを指す。コンテンツは、問題があると思われるものを特定するために全てスキャンされる。

現在、CSSをめぐる議論は、主に子どもの性的虐待（CSAM）の検出に焦点が当てられている。

しかし、クライアントサイド・スキャンはあらゆるタイプのコンテンツを検出するのに利用できるため、もし実施されれば、テロリズムのような他の重大犯罪の証拠を探したり、政治的言論の検閲のような不当な目的のために使用される可能性がある。

この技術の支持者は、スキャンは暗号化されたメッセージの送信中ではなく、メッセージが復号化されるデバイス（「エンド」）で行われるため、CSSはE2EEを破壊しないと主張している。

国家による E2EE へのアクセス
事例：クライアントサイド・スキャン

- 暗号化される前のデータにアクセス
- 捜査機関などが保存しているデータベースのデータと照合
- 違法コンテンツかどうかを判別
- 現状では、EU などで子どもの性的搾取コンテンツの取り締まり目的で導入の方向
- この手法はあらゆる目的で利用可能

「たとえ精度が高くても、誤検知の多発は避けられず、それによって罪のない多数の個人が巻き込まれる。このような影響の可能性を考えると、無差別な監視は、人々が他者とのコミュニケーションや交流の方法を制限したり、自己検閲を行ったりすることで、表現の自由や結社に著しい萎縮効果をもたらす可能性が高い」（国連人権高等弁務官）

国家によるE2EEへのアクセス事例：メタデータ分析

E2EEはデータ本文は暗号化するが、通信に関連するメタデータ(IPアドレス、配送経路情報など)を保護しない

- 政府および企業の提案では、E2EE通信のメタデータを調査することにますます焦点が当てられている。
- 議論の内容を知らなくても、誰がその場にいるのか、彼らがどこにいるのかを観察することができる。
- メタデータは、特に大量に収集された場合、コンテンツと同じくらい暴露的なものとなりうる。メタデータの大量収集または解析は、全面的かつ無差別な監視形態である。
- E2EEを破るための代替手段としてメタデータを使用することは、人権の観点からは何ら好ましいものではない。

暗号化の大切さを確認しよう
世界中の抑圧された人々を防衛するためにも

プライバシー侵害や監視されることについては、実感を伴わないことが多く気づきにくい。このことを理解した上で対処することが大切になる

- 企業は営利目的で、政府は権力維持目的で、私たちの動静を把握しようとする
- 通信の秘密が保障されていない環境では、コミュニケーションの自由はありえない
- コミュニケーションで大切なことは、自分のプライバシーではなく相手のプライバシー
- 政府の政策や法律に頼らなくても、自分一人から取り組めることがいろいろある。実践することが大切です。